ERICOM
Be Connected, Be Secure

Quickly Add Zero Trust Security Controls To Your Existing VPN

Ericom Application Isolator™

Zero Trust Control for Secure Network and Remote Application Access

Excessive Trust Leads to Excessive Security Risk

Digital transformation initiatives have made today's networks vastly different from those of a decade ago. Applications and other resources are spread between datacenters and the cloud. Users expect seamless anytime access from anywhere, on any devices.

Outdated perimeter-based trust assumptions place businesses at significant risk. In the office, logged-in users have unfettered network access, VPNs likewise "trust" remote users fully once they connect and grant them similar broad network access. Especially with the growth in remote work, this unlimited reach exposes vast attack surfaces, enabling easy lateral spread when a connected device is compromised, stolen or lost.

Zero Trust Access Control for VPNs and Networks

Increased reliance on VPNs makes improved secure access an absolute must. Adopting a default-deny security posture entails enabling user access to apps and data only after trust is established. A hacker who successfully breached an organization's perimeter would face an entirely dark network, with no ability to discover or attack applications and data on it.

Based on core Zero Trust principles of "trust nothing, verify everything" and least privilege access, Ericom Application Isolators delivers Zero Trust Network Access (ZTNA) control to existing VPNs and networks. The lightweight AI-enabled software solution works with existing VPNs, is easily implemented, and is transparent to legitimate users.

A Simple Security Boost for VPNs and Corporate Networks

Ericom Application Isolator eliminates over-privileged access to dramatically shrink enterprise network attack surfaces. Users who connect remotely via a VPN or via an internal network connection can access only the specific applications they are authorized to use, only after their identity has been authenticated. Application isolation dramatically strengthens security by "cloaking" resources so their DNS information and IP ports are not exposed.

Fast, Lightweight and Affordable

Ericom Application Isolator integrates seamlessly with your existing VPN and firewalls. The software is simple to install, requiring no endpoint installation. With no user training needed, the move to Zero Trust security is easy and fast.

Hands-free Granular Policy Generation

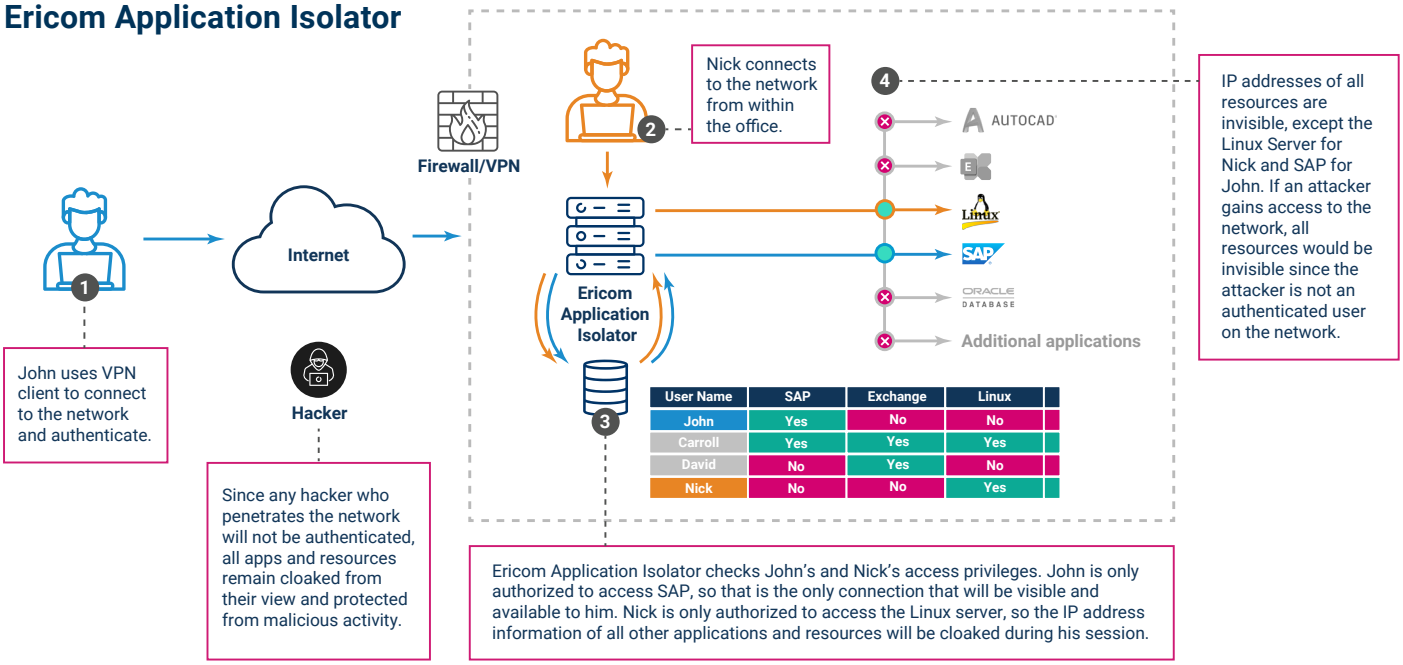
Ericom Application Isolator takes the pain out of creating granular policies for even thousands of users. Least privilege permission policies can be automatically created based on network analysis of traffic patterns for each individual, and easily adjust as user needs change.

Application Isolation at a Glance

- Adds Zero Trust Network Access controls to your existing VPN and network
- Cloaks applications to shrink network attack surface -- attackers cannot attack what they don't see
- Authorizes user access at application level to dramatically improve security posture
- Patent-pending automatic granular application access policy generation simplifies move to Zero Trust
- Addresses "north-south" and "east-west" application access risk scenarios
- Integrates with leading VPNs and firewalls to provide seamless user experience
- Transparent to users, who log on and access apps as usual
- High availability design is resilient and scales easily
- Simple deployment and management

ERICOM
BE CONNECTED, BE SECURE

Ericom Application Isolator



User Name	SAP	Exchange	Linux
John	Yes	No	No
Carroll	Yes	Yes	Yes
David	No	Yes	No
Nick	No	No	Yes

	STANDARD Core Zero Trust access capabilities for your VPN.	ADVANCED Advanced features for larger organizations.
Application isolation for remote access	✓	✓
Application cloaking	✓	✓
Application access auditing	✓	✓
Automated access policy creation		✓
Application isolation for internal access		✓
Geolocation access blocking		✓
Time-of-day access blocking		✓
Tech support	Online Resources	Business Hours

Auto Policy Manager

Ericom Application Isolator automatically generates granular, least-privilege user access policies across entire organizations based on AI-enabled network traffic analysis. User and group policies may include per-resource restrictions on access times, locations and additional factors. Policies may be easily adjusted or overridden as needed.

V.04.8.a

About Ericom Software www.ericom.com

Ericom Software provides businesses with secure access to the web and corporate applications, in the cloud and on-premises, from any device or location. Leveraging innovative isolation capabilities and multiple secure access technologies, Ericom's solutions ensure that devices and applications are protected from cybersecurity threats, and users can connect to only the specific resources they are authorized to access.

Americas:
T +1 (201)767-2210
E-mail: info@ericom.com

UK & Western Europe:
T +44 (0)1905 777970
E-mail: ukinfo@ericom.com

Worldwide:
T +972-2-591-1700
E-mail: info@ericom.com

Follow us